Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, therefore the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
ACNews	A vulnerability has been reported in ACNews that could let remote malicious users disclose sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	ACNews Information Disclosure CAN-2005-2677	Medium	Security Tracker, Alert ID: 1014749, August 22, 2005
Cisco CiscoWorks Monitoring Center for Security 1.2 to 2.1	A vulnerability has been reported in CiscoWorks Monitoring Center for Security and CiscoWorks Management Center for IDS Sensors that could let local malicious users spoof or disclose information. Vendor patch available:	CiscoWorks Information Spoofing or Disclosure	Medium	Cisco Security Advisory, ID: 66142, August 22, 2005

CiscoWorks Management Center for IDS Sensors 2.0, 2.1	http://www.cisco.com/ pcgi-bin/tablebuild.pl/ mgmt-ctr-ids-app Currently we are not aware of any exploits for these vulnerabilities.			
Ivory.org Whisper 32 1.16	A vulnerability has been reported in Whisper 32 that could let local malicious users disclose password information. No workaround or patch available at time of publishing. There is no exploit code required.	Whisper 32 Password Disclosure CAN-2005-2664	Medium	Security Tracker, Alert ID: 1014730, August 18, 2005
Microsoft Internet Explorer 5.5, 6	A vulnerability has been reported in Internet Explorer ('msdds.dll' COM Object) that could let remote malicious users execute arbitrary code. Vendor workarounds available: http://www.microsoft.com/ technet/security/ advisory/906267.mspx An exploit script has been published.	Internet Explorer Arbitrary Code Execution CAN-2005-2127	High	Microsoft Security Advisory 906267, August 18, 2005 US-CERT VU#740372
Microsoft Plug and Play	A vulnerability has been reported in Plug and Play that could let local or remote malicious users execute arbitrary code or obtain elevated privileges. Vendor fix available: http://www.microsoft.com/ technet/security/Bulletin /MS05-039.mspx **Vendor has provided additional information:** **http://www.microsoft.com/ technet/security/ advisory/906574.mspx** Exploit scripts have been published and worm, "Worm:Win32/Zotob.A", is circulating.	Microsoft Plug and Play Arbitrary Code Execution or Elevated Privileges CAN-2005-1983	High	Microsoft Security Bulletin MS05-039, August 9, 2005 US-CERT VU#998653 Microsoft Security Advisory, 899588, August 15, 2005 **Microsoft Security Advisory, 906574, August 23, 3005**
Moneymaker Gaming Chris Moneymaker's World Poker Championship V1.0	A buffer overflow vulnerability has been reported in Chris Moneymaker's World Poker Championship that could let remote malicious users execute arbitrary code. Vendor will not be creating a bugfix for this issue. There is no exploit code required; however, a Proof of Concept exploit script has been published.	Chris Moneymaker's World Poker Championship Arbitrary Code Execution CAN-2005-2639	High	Security Tracker, Alert ID: 1014738, August 19, 2005
Nortel VPN Client 4.86_033, 4.91_021, 5.01_030	A vulnerability has been reported in VPN Client that could let local malicious users obtain elevated privileges. Contact vendor for upgrade to version 5.01_103. There is no exploit code required.	Nortel VPN Client Privilege Elevation CAN-2005-2579	Medium	Nortel Security Advisory 2005006143 V2, August 18, 2005
Sysinternals Process Explorer 9.23	A buffer overflow vulnerability has been reported in Process Explorer that could let remote malicious users execute arbitrary code. Update available at: http://www.sysinternals.com/ Utilities/ProcessExplorer.html There is no exploit code required; however, Proof of Concept exploits have been published.	Process Explorer Arbitrary Code Execution CAN-2005-2679	High	Security Tracker Alert ID: 1014742, August 19, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Adobe Version Cue 1.0.1, 1.0	A vulnerability has been reported due to insecure file permissions on internal Version Cue application files, which could let a malicious user obtain elevated privileges. Patches available at: http://www.adobe.com/ support/downloads/ detail.jsp?ftpID=2985 Currently we are not aware of any exploits for this vulnerability.	Adobe Version Cue for Mac OS X Elevated Privileges CAN-2005-1842 CAN-2005-1843	Medium	Security Focus, Bugtraq ID: 14638, August 23, 2005

Apple MacOS X 10.3.9, 10.4.2	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported in AppKit, which could let a remote malicious user execute arbitrary code via a crafted Rich Text Format (RTF) file; a buffer overflow vulnerability was reported in AppKit, which could let a remote malicious user execute arbitrary code via a crafted Microsoft Word file; a buffer overflow vulnerability has been reported in the Directory Service's authentication process, which could let a remote malicious user execute arbitrary code; a vulnerability was reported in Safari when rendering Rich Text Format (RTF) files, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability was reported in 'servermgrd,' which could let a remote malicious user execute arbitrary code during authentication; and a vulnerability was reported in Safari WebKit when directly accessing URLs that are in PDF files without normal security checks, which could let a remote malicious user execute arbitrary code; Update information available at: http://docs.info.apple.com/ article.html?artnum=302163 Currently we are not aware of any exploits for these vulnerabilities.	Apple Mac OS X Multiple Arbitrary Code Execution Vulnerabilities CAN-2005-2501 CAN-2005-2502 CAN-2005-2507 CAN-2005-2516 CAN-2005-2518 CAN-2005-2522	High	Apple Security Update 2005-007, APPLE-SA-2005-08-15, US-CERT VU#172948 US-CERT VU#435188 US-CERT VU#913820 US-CERT VU#709220 US-CERT VU#461412 US-CERT VU#420316
BlueZ BlueZ 2.18 & prior	A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.bluez.org/ redirect.php?url= http%3A%2F%2F bluez.sf.net%2F down load%2F bluez-libs-2.19.tar.gz Gentoo: http://security.gentoo.org/ glsa/glsa-200508-09.xml **Debian:** **http://security.debian.org/ pool/updates/contrib/ b/bluez-utils/** There is no exploit code required.	BlueZ Arbitrary Command Execution CAN-2005-2547	High	Security Focus 14572, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-09, August 17, 2005 **Debian Security Advisory, DSA 782-1, August 23, 2005**
Clam AntiVirus 0.86.1	Multiple vulnerabilities have been reported in Clam AntiVirus that could let remote malicious users cause a Denial of Service. Upgrade to version 0.86.2: http://www.clamav.net/ stable.php#pagestart Conectiva: ftp://atualizacoes. conectiva.com.br/ Mandriva: http://www.mandriva.com/ security/advisories?name= MDKSA-2005:125 Gentoo: http://security.gentoo.org/ glsa/glsa-200507-25.xml SUSE: ftp://ftp.suse.com /pub/suse/ **Debian:** **http://security.debian.org/ pool/updates/main /c/clamav/** Currently we are not aware of any exploits for these vulnerabilities.	Clam AntiVirus Multiple Vulnerabilities CAN-2005-2450	Low	Secunia, Advisory: SA16180, July 25, 2005 Gentoo Linux Security Advisory GLSA 200507-25, July 26, 2005 Mandriva Security Advisory, MDKSA-2005:125, July 27, 2005 SUSE Security Summary Report, SUSE-SR:2005:018, July 28, 2005 Conectiva Linux Announcement, CLSA-2005:987, July 29, 2005 **Debian Security Advisory, DSA 776-1, August 16, 2005**
Elm Development Group ELM 2.5.5-2.5.7	A buffer overflow vulnerability has been reported due to insufficient parsing of SMTP 'Expires' header lines, which could let a remote malicious user execute arbitrary code. Update to Elm 2.5 PL8 available at: ftp://ftp.virginia.edu /pub/elm/ An exploit script has been published.	Elm 'Expires' Header Remote Buffer Overflow CAN-2005-2665	High	Security Tracker Alert ID: 1014745, August 20, 2005

Eric Raymond Fetchmail 6.2.5	A remote buffer overflow vulnerability has been reported in the POP3 client due to insufficient boundary checks, which could let a malicious user obtain elevated privileges. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Redhat: http://rhn.redhat.com/errata/RHSA-2005-640.html Ubuntu: http://www.ubuntulinux.org/support/ documentation/usn/usn-153-1 Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200507-21.xml Debian: http://security.debian.org/pool/updates/main/f/fetchmail/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for this vulnerability.	Fetchmail POP3 Client Buffer Overflow CAN-2005-2335	Medium	Fedora Update Notifications, FEDORA-2005-613 & 614, July 21, 2005 Redhat Security Advisory, RHSA-2005:640-08, July 25, 2005 Ubuntu Security Notice, USN-153-1, July 26, 2005 Gentoo Security Advisory, GLSA 200507-21, July 25, 2005 Debian Security Advisory, DSA 774-1, August 12, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 **Turbolinux Security Advisory, TLSA-2005-84, August 18, 2005**
GNU cpio 1.0-1.3, 2.4.2, 2.5, 2.5.90, 2.6	A vulnerability has been reported when an archive is extracted into a world or group writeable directory because non-atomic procedures are used, which could let a malicious user modify file permissions. Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-378.html **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32** There is no exploit code required.	CPIO CHMod File Permission Modification CAN-2005-1111	Medium	Bugtraq, 395703, April 13, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005: 116, July 12, 2005 RedHat Security Advisory, RHSA-2005:378-17, July 21, 2005 **SGI Security Advisory, 20050802-01-U, August 15, 2005** **SCO Security Advisory, SCOSA-2005.32, August 18, 2005**
GNU cpio 2.6	A Directory Traversal vulnerability has been reported when invoking cpio on a malicious archive, which could let a remote malicious user obtain sensitive information. Gentoo: http://security.gentoo.org/glsa/glsa-200506-16.xml Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories **SCO:**	CPIO Directory Traversal CAN-2005-1229	Medium	Bugtraq, 396429, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200506-16, June 20, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0030, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA2005: 116, July 12, 2005 **SCO Security Advisory,**

	ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.32 A Proof of Concept exploit has been published.			**SCOSA-2005.32, August 18, 2005**
GNU shtool 2.0.1 & prior	A vulnerability has been reported that could let a local malicious user gain escalated privileges. The vulnerability is caused due to temporary files being created insecurely. Gentoo: http://security.gentoo.org/glsa/glsa-200506-08.xml OpenPKG: ftp://ftp.openpkg.org/release/2.3 RedHat: http://rhn.redhat.com/errata/RHSA-2005-564.html Trustix: http://http.trustix.org/pub/trustix/updates/ SGI: http://www.sgi.com/support/security/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/php4/** There is no exploit code required.	GNU shtool Insecure Temporary File Creation CAN-2005-1751	Medium	Secunia Advisory, SA15496, May 25, 2005 Gentoo Linux Security Advisory, GLSA 200506-08, June 11, 200 OpenPKG Security Advisory, OpenPKG-SA-2005.011, June 23, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0036, July 14, 2005 SGI Security Advisory, 20050703-01-U, July 15, 2005 **Ubuntu Security Notice, USN-171-1, August 20, 2005**
HAURI Inc. ViRobot Linux Server 2.0, ViRobot Expert 4.0 , ViRobot Advanced Server, Hauri LiveCall	Several vulnerabilities have been reported: a Directory Traversal vulnerability was reported due to insufficient validation of filenames in compressed archives before extracting into a temporary directory, which could let a remote malicious user write files to arbitrary directories on the target system; and a buffer overflow vulnerability was reported in the ACE archive decompression library (vrAZace.dll) due to a boundary error, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.globalhauri.com/html/download/down_unixpatch.html There is no exploit code required.	HAURI Anti-Virus Compressed Files Directory Traversal & Buffer Overflow CAN-2005-2670 CAN-2005-2671	High	Security Tracker Alert ID: 1014740, August 20, 2005
KDE KDE 3.0 - 3.4.2	A vulnerability was reported in 'langen2kvtml' due to the insecure creation of temporary files, which could let malicious user obtain elevated privileges. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	KDE langen2kvtml Insecure Temporary File Creation CAN-2005-2101	Medium	KDE Security Advisory, August 15, 2005 Fedora Update Notification, FEDORA-2005-745, August 15, 2005 **Fedora Update Notifications, FEDORA-2005-744 & 745, August 16, 2005**
lm_sensors lm_sensors 2.9.1	A vulnerability has been reported in the 'pwmconfig' script due to the insecure creation of temporary files, which could result in a loss of data or a Denial of Service. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lm-sensors/ There is no exploit code required.	LM_sensors PWMConfig Insecure Temporary File Creation CAN-2005-2672	Low	Security Focus, Bugtraq ID: 14624, August 22, 2005 Ubuntu Security Notice, USN-172-1, August 23, 2005

MediaWiki MediaWiki 1.4.5	A vulnerability has been reported in MediaWiki that could let remote malicious users perform Cross-Site Scripting attacks. Update to version 1.4.6: http://sourceforge.net/project/showfiles.php?group_id=34373 **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	MediaWiki Cross Site Scripting CAN-2005-2215	Medium	Security Focus, 14181, July 7, 2005 **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
Mike Kershaw Kismet 2005-07-R1	Multiple vulnerabilities have been reported: an integer underflow vulnerability was reported when handling pcap files; a vulnerability was reported due to an unspecified error when handling non-printable characters in SSID; and a integer underflow vulnerability was reported in the data frame dissection, which could possibly lead to the execution of arbitrary code. Upgrade available at: http://www.kismetwireless.net/code/kismet-2005-08-R1.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200508-10.xml Currently we are not aware of any exploits for these vulnerabilities.	Kismet Multiple Remote Vulnerabilities CAN-2005-2626 CAN-2005-2627	High	Security Focus, Bugtraq ID 14430, August 16, 2005 Gentoo Linux Security Advisory, GLSA 200508-10, August 19, 2005

Multiple Vendors
Glyph and Cog Xpdf 3.0, pl2 & pl3;
Ubuntu Linux 5.0 4 powerpc, i386, amd64;
RedHat Enterprise Linux WS 4, ES 4, AS 4, Desktop 4.0;
KDE 3.4.1, 3.4, 3.3.1, 3.3.2;
GNOME GPdf 2.8.3, 2.1
	A remote Denial of Service vulnerability has been reported when verifying malformed 'loca' table in PDF files.
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-670.html
	http://rhn.redhat.com/errata/RHSA-2005-671.html
	http://rhn.redhat.com/errata/RHSA-2005-708.html
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/x/xpdf/
	KDE:
	http://www.kde.org/info/security/advisory-20050809-1.txt
	Mandriva:
	http://www.mandriva.com/security/advisories
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200508-08.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
	Debian:
	http://security.debian.org/pool/updates/main/k/kdegraphics/
	Currently we are not aware of any exploits for this vulnerability.
		XPDF Loca Table Verification Remote Denial of Service
		CAN-2005-2097
			Low	RedHat Security Advisories, RHSA-2005:670-05 & RHSA-2005:671-03, & RHSA-2005:708-05, August 9, 2005
				Ubuntu Security Notice, USN-163-1, August 09, 2005
				KDE Security Advisory, 20050809-1, August 9, 2005
				Mandriva Linux Security Update Advisories, MDKSA-2005:134, 135, 136 & 138, August 11, 2005
				SGI Security Advisory, 20050802-01-U, August 15, 2005
				Gentoo Linux Security Advisory GLSA, 200508-08, August 16, 2005
				Fedora Update Notifications, FEDORA-2005-729, 730, 732, & 733, August 15 & 17, 2005
				Debian Security Advisory, DSA 780-1, August 22, 2005

Multiple Vendors SuSE Linux Professional 9.3, x86_64, 9.2, x86_64, Linux Personal 9.3, x86_64; Linux kernel 2.6-2.6.12	A buffer overflow vulnerability has been reported in the XFRM network architecture code due to insufficient validation of user-supplied input, which could let a malicious user execute arbitrary code. Patches available at: http://www.kernel.org/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel XFRM Array Index Buffer Overflow CAN-2005-2456	High	Security Focus, 14477, August 5, 2005 **Ubuntu Security Notice, USN-169-1, August 19, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1, 1.2 .0.7, 1.1-1.1.4, 1.0-1.0.9; Ubuntu Linux 5.0 4, powerpc, i386, amd64, 4.1 ppc, ia64, ia32; SuSE Open-Enterprise-Server 9.0, Novell Linux Desktop 9.0, Linux Professional 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Personal 9.3, x86_64, 9.2, x86_64, 9.1, x86_64, Linux Enterprise Server 9; Gentoo Linux; FreeBSD 5.4, -RELENG, -RELEASE, -PRERELEASE, 5.3, -STABLE, -RELENG, -RELEASE; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; zsync 0.4, 0.3-0.3.3, 0.2-0.2.3 , 0.1-0.1.6 1, 0.0.1-0.0.6	A buffer overflow vulnerability has been reported due to insufficient validation of input data prior to utilizing it in a memory copy operation, which could let a remote malicious user execute arbitrary code. Debian: ftp://security.debian.org/pool/updates/main/z/zlib/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:16/zlib.patch Gentoo: http://security.gentoo.org/glsa/glsa-200507-05.xml SUSE: ftp://ftp.suse.com/pub/suse/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ Mandriva: http://www.mandriva.com/security/advisories OpenBSD: http://www.openbsd.org/errata.html OpenPKG: ftp.openpkg.org RedHat: http://rhn.redhat.com/errata/RHSA-2005-569.html Trustix: http://http.trustix.org/pub/trustix/updates/ Slackware: ftp://ftp.slackware.com/pub/slackware/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ zsync: http://prdownloads.sourceforge.net/zsync/zsync-0.4.1.tar.gz?download Apple: http://docs.info.apple.com/article.html?artnum=302163 **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33** Currently we are not aware of any exploits for this vulnerability.	Zlib Compression Library Buffer Overflow CAN-2005-2096	High	Debian Security Advisory DSA 740-1, July 6, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:16, July 6, 2005 Gentoo Linux Security Advisory, GLSA 200507-05, July 6, 2005 SUSE Security Announcement, SUSE-SA:2005:039, July 6, 2005 Ubuntu Security Notice, USN-148-1, July 06, 2005 RedHat Security Advisory, RHSA-2005:569-03, July 6, 2005 Fedora Update Notifications, FEDORA-2005-523, 524, July 7, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:11, July 7, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.013, July 7, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0034, July 8, 2005 Slackware Security Advisory, SSA:2005-189-01, July 11, 2005 Turbolinux Security Advisory, TLSA-2005-77, July 11, 2005 Fedora Update Notification, FEDORA-2005-565, July 13, 2005 SUSE Security Summary Report, SUSE-SR:2005:017, July 13, 2005 Security Focus, 14162, July 21, 2005 USCERT Vulnerability Note VU#680620, July 22, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 **SCO Security Advisory, SCOSA-2005.33, August 19, 2005**

Multiple Vendors zlib 1.2.2, 1.2.1; Ubuntu Linux 5.04 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Debian Linux 3.1 sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha	A remote Denial of Service vulnerability has been reported due to a failure of the library to properly handle unexpected compression routine input. Zlib: http://www.zlib.net/zlib-1.2.3.tar.gz Debian: http://security.debian.org/pool/updates/main/z/zlib/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zlib/ OpenBSD: http://www.openbsd.org/errata.html#libz2 Mandriva: http://www.mandriva.com/security/ advisories?name=MDKSA-2005:124 Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.323596 FreeBSD: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:18.zlib.asc SUSE: http://lists.suse.com/archive/suse-security-announce/2005-Jul/0007.html Gentoo: http://security.gentoo.org/glsa/glsa-200507-28.xml http://security.gentoo.org/glsa/glsa-200508-01.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Apple:** **http://docs.info.apple.com/article.html?artnum=302163** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/Server/10/updates/** **SCO:** **ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor Zlib Compression Library Decompression Remote Denial of Service CAN-2005-1849	Low	Security Focus, Bugtraq ID 14340, July 21, 2005 Debian Security Advisory DSA 763-1, July 21, 2005 Ubuntu Security Notice, USN-151-1, July 21, 2005 OpenBSD, Release Errata 3.7, July 21, 2005 Mandriva Security Advisory, MDKSA-2005:124, July 22, 2005 Secunia, Advisory: SA16195, July 25, 2005 Slackware Security Advisory, SSA:2005-203-03, July 22, 2005 FreeBSD Security Advisory, SA-05:18, July 27, 2005 SUSE Security Announcement, SUSE-SA:2005:043, July 28, 2005 Gentoo Linux Security Advisory, GLSA 200507-28, July 30, 2005 Gentoo Linux Security Advisory, GLSA 200508-01, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Conectiva Linux Announcement, CLSA-2005:997, August 11, 2005 **Apple Security Update, APPLE-SA-2005-08-15, August 15, 2005** **Turbolinux Security Advisory , TLSA-2005-83, August 18, 2005** **SCO Security Advisory, SCOSA-2005.33, August 19, 2005**

Multiple Vendors
FileZilla Server 0.7, 0.7.1;
OpenBSD -current, 3.5;
OpenPKG Current, 2.0, 2.1;
zlib 1.2.1
	A remote Denial of Service vulnerability exists during the decompression process due to a failure to handle malformed input.
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200408-26.xml
	FileZilla:
	http://sourceforge.net/project/showfiles.php?group_id=21558
	OpenBSD:
	ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.5/common/017_libz.patch
	OpenPKG:
	ftp ftp.openpkg.org
	Trustix:
	ftp://ftp.trustix.org/pub/trustix/updates/
	SuSE:
	ftp://ftp.suse.com/pub/suse/
	Mandrake:
	http://www.mandrakesecure.net/en/ftp.php
	Conectiva:
	ftp://atualizacoes.conectiva.com.br/
	SCO:
	ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2004.17
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/
	FedoraLegacy:
	http://download.fedoralegacy.org/fedora/1/updates/
	SCO:
	ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.33
	We are not aware of any exploits for this vulnerability.
		Zlib Compression Library Remote Denial of Service
		CAN-2004-0797
			Low	Security Focus, August 25, 2004
				SUSE Security Announcement, SUSE-SA:2004:029, September 2, 2004
				Mandrakelinux Security Update Advisory, MDKSA-2004:090, September 8, 2004
				Conectiva Linux Security Announcement, CLA-2004:865, September 13, 2004
				US-CERT VU#238678, October 1, 2004
				SCO Security Advisory, SCOSA-2004.17, October 19, 2004
				Conectiva Linux Security Announcement, CLA-2004:878, October 25, 2004
				Fedora Update Notification, FEDORA-2005-095, January 28, 2005
				Fedora Legacy Update Advisory, FLSA:2043, February 24, 2005
				SCO Security Advisory, SCOSA-2005.33, August 19, 2005

Multiple Vendors Linux Kernel 2.6 up to & including 2.6.12-rc4	Several vulnerabilities have been reported: a vulnerability was reported in raw character devices (raw.c) because the wrong function is called before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space; and a vulnerability was reported in the 'pkt_ioctl' function in the 'pktcdvd' block device ioctl handler (pktcdvd.c) because the wrong function is called before passing an ioctl to the block device, which could let a malicious user execute arbitrary code. Update available at: http://kernel.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-420.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** A Proof of Concept Denial of Service exploit script has been published.	Multiple Vendor Linux Kernel pktcdvd & raw device Block Device CAN-2005-1264 CAN-2005-1589	High	Secunia Advisory, SA15392, May 17, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:110, July 1, 2005 RedHat Security Advisory, RHSA-2005:420-24, Updated August 9, 2005 **Conectiva Linux Announcement, CLSA-2005:999, August 17, 2005**

Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available at: http://kernel.org/ Trustix: http://www.trustix.org/errata/2005/0022/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-472.html Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-120_RHSA-2005-283_RHSA-2005-284_RHSA-2005-293_RHSA-2005-472.pdf SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ Mandriva: http://www.mandriva.com/security/advisories **Conectiva:** **ftp://atualizacoes.conectiva.com.br/10/** An exploit script has been published.	Linux Kernel ELF Core Dump Buffer Overflow CAN-2005-1263	High	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 RedHat Security Advisory, RHSA-2005:472-05, May 25, 2005 Avaya Security Advisory, ASA-2005-120, June 3, 2005 Trustix Secure Linux Bugfix Advisory, TSLSA-2005-0029, June 24, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:110 & 111, June 30 & July 1, 3005 **Conectiva Linux Announcement, CLSA-2005:999, August 17, 2005**
Multiple Vendors Linux kernel 2.6-2.6.12 .1	A vulnerability has been reported due to insufficient authorization before accessing a privileged function, which could let a malicious user bypass IPSEC policies. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel IPSec Policies Authorization Bypass CAN-2005-2555	Medium	Ubuntu Security Notice, USN-169-1, August 19, 2005 Security Focus, Bugtraq ID 14609, August 19, 2005
Multiple Vendors Linux kernel 2.6-2.6.12 .1	Several vulnerabilities have been reported: a Denial of Service vulnerability was reported due to an error when handling key rings; and a Denial of Service vulnerability was reported in the 'KE YCTL_JOIN_SESSION _KEYRING' operation due to an error when attempting to join a key management session. Patches available at: http://kernel.org/pub/linux/kernel/v2.6/snapshots/patch-2.6.13-rc6-git 1.bz2 **Outhunt:** **http://security.ubuntu.com/ubuntu/pool/main/l/** There is no exploit code required.	Linux Kernel Management Denials of Service CAN-2005-2098 CAN-2005-2099	Low	Secunia Advisory: SA16355, August 9, 2005 **Ubuntu Security Notice, USN-169-1, August 19, 2005**
Multiple Vendors ncpfs 2.2.1 - 2.2.4	A buffer overflow exists that could lead to local execution of arbitrary code with elevated privileges. The vulnerability is in the handling of the '-T' option in the ncplogin and ncpmap utilities, which are both installed as SUID root by default. Gentoo: Update to 'net-fs/ncpfs-2.2.5' or later http://www.gentoo.org/security/en/glsa/glsa-200412-09.xml SUSE: Apply updated packages. Updated packages are available via YaST Online Update or the SUSE FTP site.	Multiple Vendors ncpfs: ncplogin and ncpmap Buffer Overflow CAN-2004-1079	High	Gentoo Linux Security Advisory, GLSA 200412-09 / ncpfs, December 15, 2004 Secunia SA13617, December 22, 2004 Mandrakelinux Security Update Advisory, MDKSA-2005:028, February 2, 2005 **Fedora Update**

	Mandrake: http://www.mandrakesecure.net/en/ftp.php **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.			**Notification FEDORA-2005-435, August 16, 2005**
Multiple Vendors Novell Evolution 2.0.2-2.0.4; LibTIFF 3.6.1; sy Software Products CUPS 1.1.12-1.1.23, 1.1.10, 1.1.7, 1.1.6, 1.1.4 -5, 1.1.4-3, 1.1.4 -2, 1.1.4, 1.1.1, 1.0.4 -8, 1.0.4; Ubuntu 4.10, 5.04	A remote Denial of Service vulnerability has been reported due to insufficient validation of specific header values. Libtiff: http://freshmeat.net/redir/libtiff/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/t/tiff/ **Mandriva:** **http://www.mandriva.com/security/advisories** A Proof of Concept exploit has been published.	LibTiff Tiff Image Header Remote Denial of Service CAN-2005-2452	Low	Security Focus Bugtraq ID 14417, July 29, 2005 Ubuntu Security Notice, USN-156-1, July 29, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:142, August 18, 2005**
Multiple Vendors Ubuntu Linux 4.1 ppc, ia64, ia32; Linux kernel 2.6.8, rc1&rc2	A remote Denial of Service vulnerability has been reported when handling UDP packets received by SNMPD due to a NULL pointer dereference. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel SNMP Handler Remote Denial of Service CAN-2005-2548	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Linux kernel 2.6.10, rc2, 2.6.8, rc1	A remote Denial of Service vulnerability has been reported in the kernel driver for compressed ISO file systems when attempting to mount a malicious compressed ISO image. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel ISO File System Remote Denial of Service CAN-2005-2457	Low	Ubuntu Security Notice, USN-169-1, August 19, 2005

Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; Rob Flynn Gaim 1.3.1, 1.3 .0, 1.2.1, 1.2 , 1.1.1 -1.1.4, 1.0-1.0.2; RedHat Enterprise Linux WS 2.1, IA64, ES 2.1, IA64, AS 2.1, IA64, Desktop 4.0, Advanced Workstation for the Itanium Processor 2.1, IA64	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported due to the way away messages are handled, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability has been reported due to an error when handling file transfers. Updates available at: http://gaim.sourceforge.net/downloads.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-589.html http://rhn.redhat.com/errata/RHSA-2005-627.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-06.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** A Proof of Concept exploit has been published for the buffer overflow vulnerability.	Gaim AIM/ICQ Protocols Buffer Overflow & Denial of Service CAN-2005-2102 CAN-2005-2103	High	RedHat Security Advisories, RHSA-2005:589-16 & RHSA-2005:627-11, August 9, 2005 Ubuntu Security Notice, USN-168-1, August 12, 2005 Gentoo Linux Security Advisory, GLSA 200508-06, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:139, August 16, 2005 **Fedora Update Notifications, FEDORA-2005-750 & 751, August 17, 2005** **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64, 4.1 ppc, ia64, ia32; GNOME Evolution 2.3.1 -2.3.6 .1, 2,0- 2.2 , 1.5	Multiple format string vulnerabilities have been reported: a vulnerability was reported when vCard information is attached to an email message, which could let a remote malicious user execute arbitrary code; a vulnerability was reported when specially crafted contact data that has been retrieved from an LDAP server is displayed, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported when specially crafted task list data that has been retrieved from remote servers and the data has been saved under the 'Calendars' tab is displayed, which could let a remote malicious user execute arbitrary code. Updates available at: http://ftp.gnome.org/pub/gnome/sources/evolution/2.3/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ **Mandriva:** **http://www.mandriva.com/security/advisories** **SUSE:** **ftp://ftp.suse.com/pub/suse/** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-12.xml** Currently we are not aware of any exploits for these vulnerabilities.	GNOME Evolution Multiple Format String CAN-2005-2549 CAN-2005-2550	High	Secunia Advisory: SA16394, August 11, 2005 Ubuntu Security Notice, USN-166-1, August 11, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:141, August 18, 2005** **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005** **Gentoo Linux Security Advisory, GLSA 200508-12, August 23, 2005**
Mutt Mutt 1.5.10	A buffer overflow vulnerability has been reported in 'Handler.c' in the 'mutt_decode_xbit() function,' which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Mutt Handler.c Buffer Overflow CAN-2005-2642	High	Security Tracker Alert ID: 1014729, August 18, 2005

netpbm 10.0	A vulnerability has been reported in netpbm ('-dSAFER') that could let malicious users execute arbitrary postscript code. Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200508-04.xml Mandriva: http://www.mandriva.com/security/advisories Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netpbm-free/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** **SUSE:** **ftp://ftp.suse.com/pub/suse/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-743.html** There is no exploit code required.	netpbm Arbitrary Code Execution CAN-2005-2471	High	Secunia Advisory: SA16184, July 25, 2005 Trustix Secure Linux Security Advisory, #2005-0038, July 29, 2005 Gentoo Linux Security Advisory, GLSA 200508-04, August 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:133, August 10, 2005 Ubuntu Security Notice, USN-164-1, August 11, 2005 **Fedora Update Notifications, FEDORA-2005-727 & 728, August 17, 2005** **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005** **RedHat Security Advisory, RHSA-2005:743-08, August 22, 2005**
PCRE PCRE 6.1, 6.0 , 5.0	A vulnerability has been reported in 'pcre_compile.c' due to an integer overflow, which could let a remote/local malicious user potentially execute arbitrary code. Updates available at: http://www.pcre.org/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/pcre3/ Currently we are not aware of any exploits for this vulnerability.	PCRE Regular Expression Heap Overflow CAN-2005-2491	High	Secunia Advisory: SA16502, August 22, 2005 Ubuntu Security Notice, USN-173-1, August 23, 2005
Petr Vandrovec ncpfs prior to 2.2.6	Two vulnerabilities exist: a vulnerability exists in 'ncpfs-2.2.0.18/lib/ncplib.c' due to improper access control in the 'ncp_fopen_nwc()' function, which could let a malicious user obtain unauthorized access; and a buffer overflow vulnerability exists in 'ncpfs-2.2.5/sutil/ncplogin.c' due to insufficient validation of the 'opt_set_volume_after_parsing_all_options()' function, which could let a malicious user execute arbitrary code. Update available at: ftp://platan.vc.cvut.cz/pub/linux/ncpfs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-44.xml Debian: http://www.debian.org/security/2005/dsa-665 Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-371.html **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** An exploit script has been published.	Petr Vandrovec ncpfs Access Control & Buffer Overflow CAN-2005-0013 CAN-2005-0014	High	Security Tracker Alert ID: 1013019, January 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:028, February 2, 2005 Debian Security Advisory, DSA-665-1, February 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 RedHat Security Advisory, RHSA-2005:371-06, May 17, 2005 **Fedora Update Notification FEDORA-2005-435, August 16, 2005**

ProFTPd	Multiple format string vulnerabilities have been reported in ProFTPd that could let remote malicious users cause a Denial of Service or disclose information. Upgrade to version 1.3.0rc2: http://www.proftpd.org/ Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200508-02.xml Trustix: ftp://ftp.trustix.org/pub/trustix/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for these vulnerabilities.	ProFTPD Denial of Service or Information Disclosure CAN-2005-2390	Medium	Secunia, Advisory: SA16181, July 26, 2005 Gentoo Linux Security Advisory, GLSA 200508-02, August 1, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0040, August 5, 2005 Turbolinux Security Advisory, TLSA-2005-82, August 9, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:140, August 16, 2005**
Tor Tor 0.1.0.13 & prior	A vulnerability has been reported when performing a Diffie-Hellman handshake due to a failure to reject certain weak keys, which could let a remote malicious user obtain sensitive information. Update available at: http://tor.eff.org/download.html Currently we are not aware of any exploits for this vulnerability.	Tor Weak Diffie-Hellman Handshake CAN-2005-2643	Medium	Secunia Advisory: SA16424, August 19, 2005
Vim V6.3.082	A vulnerability has been reported in Vim that could let remote malicious users execute arbitrary code. Vendor patch available: ftp://ftp.vim.org/pub/vim/patches/6.3/6.3.082 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/v/vim/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ **Mandriva:** **http://www.mandriva.com/security/advisories** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-745.html** There is no exploit code required; however, Proof of Concept exploits have been published.	Vim Arbitrary Code Execution CAN-2005-2368	High	Security Focus, 14374, July 25, 2005 Ubuntu Security Notice, USN-154-1, July 26, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0038, July 29, 2005 Fedora Update Notifications, FEDORA-2005-737, 738, & 741, August 10 & 15, 2005 Conectiva Security Advisory, CLSA-2005:995, **Mandriva Linux Security Update Advisory, MDKSA-2005:148, August 22, 2005** **RedHat Security, Advisory, RHSA-2005:745-10, August 22, 2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

Adobe Acrobat 5.x, 6.x, 7.x, Acrobat Reader 5.x, 6.x, 7.x	A buffer overflow vulnerability has been reported in the core application plug-in due to an unspecified boundary error, which could let a remote malicious user execute arbitrary code. Update information available at: http://www.adobe.com/support/techdocs/321644.html **Gentoo:** **http://security.gentoo.org/glsa/glsa-200508-11.xml** **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	Adobe Acrobat / Reader Plug-in Buffer Overflow CAN-2005-2470	High	Adobe Security Advisory, August 16, 2005 US-CERT VU#896220 **Gentoo Linux Security Advisory, GLSA 200508-11, August 19, 2005** **SUSE Security Announcement, SUSE-SA:2005:047, August 22, 2005**
Apache	A vulnerability has been reported in Apache which can be exploited by remote malicious user to smuggle http requests. Conectiva: http://distro.conectiva.com.br/ atualizacoes/index.php?id=a&anuncio=000982 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories http://security.ubuntu.com/ubuntu/pool/main/a/apache2/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SGI:** **ftp://patches.sgi.com/support/free/security/advisories/** **SuSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	Apache HTTP Request Smuggling Vulnerability CAN-2005-1268 CAN-2005-2088	Medium	Secunia, Advisory: SA14530, July 26, 2005 Conectiva, CLSA-2005:982, July 25, 2005 Fedora Update Notification FEDORA-2005-638 & 639, August 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:129, August 3, 2005 Ubuntu Security Notice, USN-160-1, August 04, 2005 Turbolinux Security Advisory, TLSA-2005-81, August 9, 2005 **SGI Security Advisory, 20050802-01-U, August 15, 2005** **SUSE Security Announcement, SUSE-SA:2005:046, August 16, 2005**
ATRC ATutor 1.5.1	A Cross-Site Scripting vulnerability has been reported in 'login.php' due to insufficient sanitization of the 'course' parameter and in 'search.php' due to insufficient sanitization of the 'words' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	ATutor Cross-Site Scripting CAN-2005-2649	Medium	Secunia Advisory: SA16496, August 19, 2005
BBCaffe BBCaffe 2.0	A Cross-Site Scripting vulnerability has been reported in several scripts due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	BBCaffe Cross-Site Scripting CAN-2005-2653	Medium	Security Focus, Bugtraq ID 14602, August 18, 2005
BEA Systems, Inc. WebLogic Portal 8.1, SP1-SP4	A vulnerability has been reported when enforcing user entitlements, which could let an unauthorized remote malicious user access entitled pages. Patches available at: ftp://ftpna.beasys.com/pub/releases/security/patch_CR238578_81SP4.zip There is no exploit code required.	BEA WebLogic Portal Access Validation CAN-2005-2680	Medium	BEA Security Advisory, BEA05-84.00, August 22, 2005
circeOS SaveWebPortal 3.4	Multiple vulnerabilities have been reported: a vulnerability was reported in the '/admin/PhpMyExplorer/editerfichier.php' script due to insufficient access restrictions, which could let a remote malicious user execute arbitrary PHP scripts; a vulnerability was reported in 'menu_dx.php' due to insufficient verification of the 'SITE_Path' parameter and in 'menu_sx.php' due to insufficient verification of the 'CONTENTS_Dir' parameter before used to include files, which could let a remote malicious user include arbitrary files; a vulnerability was reported in	SaveWebPortal Multiple Vulnerabilities	High	Secunia Advisory: SA16522, August 23, 2005

	'footer.php' due to insufficient sanitization of the 'TABLE_Width,' 'SITE_Author_Domain,' 'SITE_Author,' and 'L_info' parameters and in 'header.php,' 'menu_dx.php,' and 'mexu_sx.php' due to insufficient sanitization of multiple parameters, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because it is possible to inject arbitrary HTML and script code via 'HTTP_REFERER' and 'HTTP_USER_AGENT ' HTTP headers. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.			
Cisco Systems Cisco Clean Access (CCA) 3.5-3.5.3, 3.4-3.4.5, 3.3 - 3.3.9	A vulnerability has been reported in the CCA Application Program Interface (API) because authentication is not performed, which could let a remote malicious user bypass security, make configuration changes, or obtain sensitive information. Patches available at: http://www.cisco.com/ pcgi-bin/tablebuild.pl/ cca-patches Currently we are not aware of any exploits for this vulnerability.	Cisco Clean Access API Access Validation CAN-2005-2631	Medium	Cisco Security Advisory, 66068, August 17, 2005
Cisco Systems Intrusion Prevention System 5.0 (1) & (2)	A vulnerability has been reported in the command line processing (CLI) logic, which could let a local/remote malicious user obtain full administrative privileges. Updates available at: http://www.cisco.com/cgi-bin/tablebuild.pl/ips5 Currently we are not aware of any exploits for this vulnerability.	Cisco Intrusion Prevention System Administrative Access CAN-2005-2681	High	Cisco Security Advisory, cisco-sa-20050824, August 21, 2005
Computer Associates Message Queuing software prior to 1.07 Build 220_13 & 1.11 Build 29_13	Multiple vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported in the Computer Associates Message Queuing (CAM) service due to an unspecified error when specially crafted packets are submitted to the TCP port; buffer overflow vulnerabilities have been reported due to unspecified boundary errors, which could lead to the execution of arbitrary code; and a vulnerability has been reported due to a failure in the CAM service to verify the legitimacy of the CAFT application, which could let a remote malicious user spoof a legitimate CAFT instance and ultimately execute arbitrary code. Upgrade information available at: http://supportconnectw.ca. com/public/ca_ common_docs/ camsecurity_notice.asp There is no exploit code required.	Computer Associates Message Queuing Multiple Vulnerabilities CAN-2005-2667 CAN-2005-2668 CAN-2005-2669	High	Computer Associates Advisory, August 19, 2005 US-CERT VU#619988
Coppermine Photo Gallery 1.3-1.3.3 , 1.2-1.2.2 b, 1.1 beta 2, 1.1 .0, 1.0 RC3	A vulnerability has been reported in 'Displayimage.php' due to insufficient sanitization of EXIF data, which could let a remote malicious user execute arbitrary script code. Upgrades available at: http://prdownloads. sourceforge.net/ coppermine/cpg1.3.4.zip There is no exploit code required.	Coppermine 'Displayimage. PHP' Script Injection CAN-2005-2676	Medium	Security Focus, Bugtraq ID: 14625, August 22, 2005
DTLink Software AreaEdit 0.4.2 , 0.4.1	A vulnerability has been reported in 'aspell_setup.php' due to insufficient sanitization of the 'dictionary' variable before used as command line arguments, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://freshmeat.net/redir/ areaedit/58526/url_tgz/ areaedit_0.4.3.tar.g z There is no exploit code required.	DTLink Software AreaEdit SpellChecker Plugin Arbitrary Command Execution CAN-2005-2682	High	Secunia Advisory: SA16511, August 22, 2005
ECW-Shop ECW-Shop 6.0.2	Several vulnerabilities have been discovered: a Cross-Site Scripting vulnerability was reported due to insufficient sanitization 'max' and 'ctg' parameters before returned to users, which could let a remote malicious user execute arbitrary HTML and script code; an SQL injection vulnerability was reported due to insufficient sanitization of the 'min' and 'max' parameters before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported because a remote malicious user can modify/reduce the cost of their shopping cart. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploit have been published.	ECW Shop Cross-Site Scripting, SQL Injection & Price Modification CAN-2005-2621 CAN-2005-2622 CAN-2005-2623	Medium	Secunia Advisory: SA16459, August 17, 2005
Emefa Guestbook Emefa Guestbook 1.2	HTML injection vulnerabilities have been reported in 'sign.asp' due to insufficient sanitization of the 'name,' 'location,' and 'email' parameters before stored as a guest book entry, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required.	Emefa Guestbook Multiple HTML Injection CAN-2005-2650	Medium	Secunia Advisory: SA16489, August 18, 2005

Ethereal Ethereal V0.10.11	Multiple dissector and zlib vulnerabilities have been reported in Ethereal that could let remote malicious users cause a Denial of Service or execute arbitrary code. Upgrade to version 0.10.12: http://www.ethereal.com/download.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandriva: http://www.mandriva.com/security/advisories RedHat: http://rhn.redhat.com/errata/RHSA-2005-687.html **SUSE:** **ftp://ftp.suse.com/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	Ethereal Denial of Service or Arbitrary Code Execution CAN-2005-2361 CAN-2005-2362 CAN-2005-2363 CAN-2005-2364 CAN-2005-2365 CAN-2005-2366 CAN-2005-2367	High	Secunia, Advisory: SA16225, July 27, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:131, August 4, 2005 RedHat Security Advisory, RHSA-2005:687-03, August 10, 2005 **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
Isemarket JaguarControl	A buffer overflow vulnerability has been reported in 'JaguarEditControl.dll' due to a boundary error, which could let a remote malicious user cause a Denial of Service and/or potentially execute arbitrary code. No workaround or patch available at time of publishing. A Denial of Service Proof of Concept exploit has been published.	Isemarket JaguarControl Buffer Overflow CAN-2005-2644	High	Security Focus Bugtraq ID 14558, August 13, 2005
mediabox404 mediabox404 1.2, 1.1	An SQL injection vulnerability has been reported in 'Login_admin_Mediabox404.php' due to insufficient sanitization of the 'User' and 'Password' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. The vendor has addressed this issue in the latest CVS version. There is no exploit code required.	Mediabox404 SQL Injection CAN-2005-2634	Medium	Secunia Advisory: SA16493, August 18, 2005
MediaWiki MediaWiki 1.x	A vulnerability has been reported due to insufficient sanitization of input passed to certain HTML attributes, which could let a remote malicious user execute arbitrary script code. Upgrades available at: http://prdownloads.sf.net/wikipedia/mediawiki-1.4.5.tar.gz?download Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200506-12.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	MediaWiki Page Template Arbitrary Code Execution CAN-2005-1888	High	Security Focus, 13861, June 6, 2005 Gentoo Security Advisory, GLSA 200506-12, June 13, 2005 **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
Mozilla.org Firefox 0.x, 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error because untrusted events generated by web content are delivered to the browser user interface; a vulnerability was reported because scripts in XBL controls can be executed even when JavaScript has been disabled; a vulnerability was reported because remote malicious users can execute arbitrary code by tricking the user into using the 'Set As Wallpaper' context menu on an image URL that is really a javascript; a vulnerability was reported in the 'InstallTrigger.install()' function due to an error in the callback function, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to an error when handling 'data:' URL that originates from the sidebar, which could let a remote malicious user execute arbitrary code; an input validation vulnerability was reported in the 'InstallVersion.compareTo()' function when handling unexpected JavaScript objects, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because it is possible for remote malicious user to steal information and possibly execute arbitrary code by using standalone applications such as Flash and QuickTime to open a javascript: URL; a vulnerability was reported due to an error when handling DOM node names with different namespaces, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported due to insecure cloning of base objects, which could let a remote malicious user execute arbitrary code. Updates available at: http://www.mozilla.org/products/firefox/ Gentoo: ftp://security.gentoo.org/glsa/ Mandriva: http://www.mandriva.com/	Firefox Multiple Vulnerabilities CAN-2005-2260 CAN-2005-2261 CAN-2005-2262 CAN-2005-2263 CAN-2005-2264 CAN-2005-2265 CAN-2005-2267 CAN-2005-2269 CAN-2005-2270	High	Secunia Advisory: SA16043, July 13, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:120, July 13, 2005 Gentoo Linux Security Advisory, GLSA 200507-14, July 15, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-603 & 605, July 20, 2005 RedHat Security Advisory, RHSA-2005:586-11, July 21, 2005 Slackware Security Advisory, SSA:2005-203-01, July

	security/advisories Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates RedHat: http://rhn.redhat.com/errata/RHSA-2005-586.html Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005& m=slackware-security.418880 Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/epiphany-browser/ http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ SUSE: ftp://ftp.suse.com/pub/suse/ **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-firefox/** http://security.debian.org/pool/updates/main/m/mozilla/ SGI: ftp://patches.sgi.com/support/free/security/advisories/ Exploits have been published.		22, 2005 US-CERT VU#652366 US-CERT VU#996798 Ubuntu Security Notices, USN-155-1 & 155-2 July 26 & 28, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 SUSE Security Announcement, SUSE-SA:2005:045, August 11, 2005 Debian Security Advisory, DSA 775-1, August 15, 2005 SGI Security Advisory, 20050802-01-U, August 15, 2005 Debian Security Advisory, DSA 777-1, August 17, 2005 **Debian Security Advisory, DSA 779-1, August 20, 2005** **Debian Security Advisory, DSA 781-1, August 23, 2005**

Mozilla.org
Mozilla Browser 1.0-1.0.2, 1.1-1.7.6;
Firefox 0.8-0.10.1, 1.0.1, 1.0.2;
Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, 7.0-7.2
	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code.
	Upgrades available at:
	http://www.mozilla.org/products/firefox/
	http://www.mozilla.org/products/mozilla1.x/
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200504-18.xml
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-383.html
	http://rhn.redhat.com/errata/RHSA-2005-386.html
	TurboLinux:
	ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/
	SUSE:
	ftp://ftp.suse.com/pub/suse/
	RedHat:
	http://rhn.redhat.com/errata/RHSA-2005-384.html
	SGI:
	ftp://patches.sgi.com/support/free/security/advisories/
	Ubuntu:
	http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/
	Mandriva:
	http://www.mandriva.com/security/advisories
	FedoraLegacy:
	http://download.fedoralegacy.org/redhat/
	SCO:
	ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.29
	Gentoo:
	http://security.gentoo.org/glsa/glsa-200507-17.xml
	Fedora:
	http://download.fedora.redhat.com/pub/fedora/linux/core/updates/
		Mozilla Suite / Firefox Multiple Vulnerabilities
		CAN-2005-0752
		CAN-2005-1153
		CAN-2005-1154
		CAN-2005-1155
		CAN-2005-1156
		CAN-2005-1157
		CAN-2005-1158
		CAN-2005-1159
		CAN-2005-1160
			High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005
				Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005
				US-CERT VU#973309
				RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005
				Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005
				US-CERT VU#519317
				SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005
				RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005
				SGI Security Advisory, 20050501-01-U, May 5, 2005
				Ubuntu Security Notice, USN-124-1 & USN-124-2, May 11 & 12, 2005
				Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005
				Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005
				Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005
				Packet Storm, May 23, 2005
				SCO Security Advisory, SCOSA-2005.29, July 1, 2005
				Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005
				Fedora Update Notifications, FEDORA-2005-604 & 605, July 20, 2005
				Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005
				HP Security Bulletin, HPSBUX01133, August 8, 2005
				Debian Security Advisory, DSA 781-1, August 23, 2005

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01133 **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/** An exploit script has been published.			
Mozilla.org Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-434.html http://rhn.redhat.com/errata/RHSA-2005-435.html Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ SUSE: ftp://ftp.suse.com/pub/suse/ SGI: ftp://patches.sgi.com/support/ free/security/advisories/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01133 **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/**	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005 Ubuntu Security Notice, USN-134-1, May 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:014, June 7, 2005 SGI Security Advisory, 20050503-01-U, June 8, 2005 SUSE Security Announcement, SUSE-SA:2005:030, June 9, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 HP Security Bulletin, HPSBUX01133, August 8, 2005 **Debian Security Advisory, DSA 781-1, August 23, 2005**

	Currently we are not aware of any exploits for this vulnerability.			
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon 0.9; Netscape 7.2	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. RedHat: http://rhn.redhat.com/errata/ RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html Slackware: http://www.mozilla.org/projects/security/known-vulnerabilities.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/ TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.suse.com/pub/suse/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/ free/security/advisories/ Mandriva: http://www.mandriva.com/security/advisories FedoraLegacy: http://download.fedoralegacy.org/redhat/ SCO: ftp://ftp.sco.com/pub/updates/ UnixWare/SCOSA-2005.29 Gentoo: http://security.gentoo.org/glsa/glsa-200507-17.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/enigmail/ http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-thunderbird/ HP: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBUX01133 **Debian:** **http://security.debian.org/pool/updates/main/m/mozilla-thunderbird/** There is no exploit code required; however, a Proof of Concept exploit has been published.	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988, April 16, 2005 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 Slackware Security Advisory, SSA:2005-111-04, April 22, 2005 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005 Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005 SCO Security Advisory, SCOSA-2005.29, July 1, 2005 Gentoo Linux Security Advisory, GLSA 200507-17, July 18, 2005 Fedora Update Notifications, FEDORA-2005-604 & 605, July 20, 2005 Ubuntu Security Notices, USN-157-1 & 157-2 August 1& 2, 2005 HP Security Bulletin, HPSBUX01133, August 8, 2005 **Debian Security Advisory, DSA 781-1, August 23, 2005**

Multiple Vendors Mantis 0.19.0a-0.19.2, 0.18-0.18.3; Debian Linux 3.1, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, amd64, alpha	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability has been reported in the 'mantis/view_all_set.php' script, which could let a remote malicious user execute arbitrary HTML and nd script code; a vulnerability has been reported in 'mantis/view_all_bug_page.php' due to insufficient sanitization before returned to users, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported due to insufficient satiation of unspecified input before used in and SQL query, which could let a remote malicious user execute arbitrary SQL code. Upgrades available for the first two vulnerabilities available at: http://www.mantisbt.org/download.php Debian: http://security.debian.org/pool/updates/main/m/mantis/ There is no exploit code required.	Mantis Multiple Input Validation CAN-2005-2556 CAN-2005-2557	Medium	Debian Security Advisory, DSA 778-1, August 19, 2005 Secunia Advisory: SA16506, August 22, 2005
Multiple Vendors OpenPGP	A vulnerability exists that could permit a remote malicious user to conduct an adaptive-chosen-ciphertext attack against OpenPGP's cipher feedback mode. The flaw is due to an ad-hoc integrity check feature in OpenPGP. A solution will be available in the next release of the product. SUSE: ftp://ftp.suse.com/pub/suse/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-29.xml ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/g/gnupg/** A Proof of Concept exploit has been published.	Multiple Vendors OpenPGP CFB Mode Vulnerable to Cipher-Text Attack CAN-2005-0366	Medium	US-CERT VU#303094 SUSE Security Summary Report, SUSE-SR:2005:007, March 4, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:057, March 16, 2005 Gentoo Linux Security Advisory, GLSA 200503-29, March 24,2005 ALTLinux Security Advisory, March 29, 2005 **Ubuntu Security Notice, USN-170-1, August 19, 2005**
Multiple Vendors PHPXMLRPC 1.1.1; PEAR XML_RPC 1.3.3; Drupal 4.6-4.6.2, 4.5-4.5.4; **Nucleus CMS Nucleus CMS 3.21, 3.2, 3.1, 3.0, RC, 3.0.; MailWatch for MailScanner 1.0.1; eGroupWare 1.0.6, 1.0.3, 1.0.1, 1.0.0.007, 1.0**	A vulnerability has been reported in XML-RPC due to insufficient sanitization of certain XML tags that are nested in parsed documents being used in an 'eval()' call, which could let a remote malicious user execute arbitrary PHP code. PHPXMLRPC : http://prdownloads.sourceforge.net/phpxmlrpc/xmlrpc.1.2.tgz?download Pear: http://pear.php.net/get/XML_RPC-1.4.0.tgz Drupal: http://drupal.org/files/projects/drupal-4.5.5.tar.gz **eGroupWare:** **http://prdownloads.sourceforge.net/egroupware/eGroupWare-1.0.0.009.tar .gz?download** **MailWatch:** **http://prdownloads.sourceforge.net/mailwatch/mailwatch-1.0.2.tar.gz** **Nucleus:** **http://prdownloads.sourceforge.net/nucleuscms/**	PHPXMLRPC and PEAR XML_RPC Remote Arbitrary Code Execution CAN-2005-2498	High	Security Focus, Bugtraq ID 14560, August 15, 2995 **Security Focus, Bugtraq ID 14560, August 18, 2995** **RedHat Security Advisory, RHSA-2005:748-05, August 19, 2005** **Ubuntu Security Notice, USN-171-1, August 20, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:146, August 22, 2005**

	nucleus-xmlrpc-patch.zip ?download **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-748.html** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/p/php4/** **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.			
Multiple Vendors Ubuntu Linux 5.0 4 powerpc, i386, amd64; AWStats 6.4 & prior	A vulnerability has been reported due to insufficient sanitization of the 'url' parameter before using in an 'eval()' function when Referer field statistics are generated, which could let a remote malicious user execute arbitrary code. *Note: The system is only vulnerable if at least one URLPlugin is enabled.* Updates available at: http://awstats.sourceforge.net/files/awstats-6.4.tgz Gentoo: http://security.gentoo.org/glsa/glsa-200508-07.xml **SUSE:** **ftp://ftp.suse.com/pub/suse/** There is no exploit code required.	AWStats Arbitrary Command Execution CAN-2005-1527	High	iDEFENSE Security Advisory, August 9, 2005 Ubuntu Security Notice, USN-167-1, August 11, 2005 Gentoo Linux Security Advisory, GLSA 200508-07, August 16, 2005 **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
NetScreen ScreenOS 2.x, 3.x, 4.x, 5.x	A vulnerability has been reported because different responses are returned when a username is valid or invalid, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Netscreen VPN Username CAN-2005-2640	Medium	Security Focus, Bugtraq ID 14595, August 18, 2005
OpenVPN OpenVPN 2.0 , 1.6 .0, 1.5 .0, 1.4.0-1.4.3, 1.3.2 , 1.2.1	Multiple remote Denial of Service vulnerabilities have been reported: a Denial of Service vulnerability was reported when flushing the OpenSSL error due to a failed client certificate authentication; a Denial of Service vulnerability was reported when flushing the OpenSSL error when a received packet fails to decrypt; a Denial of Service vulnerability was reported when configured in the 'dev tap' ethernet bridging mode; and a Denial of Service vulnerability was reported when two or more clients connect to the server at the same time using the same client certificate. Upgrades available at: http://openvpn.net/release/openvpn-2.0.1.tar.gz Mandriva: http://www.mandriva.com/security/advisories There is no exploit code required.	OpenVPN Multiple Remote Denials of Service CAN-2005-2531 CAN-2005-2532 CAN-2005-2533 CAN-2005-2534	Low	Secunia Advisory: SA16463, August 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:145, August 22, 2005
phpAdsNew phpAdsNew 2.0.5	Multiple vulnerabilities have been reported: a vulnerability was reported because a vulnerable version of XML-RPC for PHP was used, which could let a remote malicious user execute arbitrary PHP code; an SQL injection vulnerability was reported in 'lib-view-direct.inc.php' due to insufficient sanitization of the 'clientid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to insufficient verification of certain parameters before used to include files, which could let a remote malicious user include arbitrary local files. The vendor has released version 2.0.6. to resolve this issue. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpAdsNew Multiple Vulnerabilities CAN-2005-2636 CAN-2005-2635 CAN-2005-2498	High	Secunia Advisory: SA16468, August 17, 2005
PHPFreeNews PHPFreeNews 1.40	Several vulnerabilities have been reported: an SQL injection vulnerability was reported in 'SearchResults.php' due to insufficient sanitization of the 'Match' and CatID' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a Cross-Site Scripting vulnerability was reported in 'SearchResults.php' and 'NewsCategoryForm.php' due to insufficient sanitization of the 'NewsMode' and 'Match' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPFreeNews SQL Injection & Cross-Site Scripting CAN-2005-2637 CAN-2005-2638	Medium	Securiteam, August 18, 2005

PHPKIT PHPKIT 1.6.1	Multiple SQL injection vulnerabilities have been reported due to insufficient sanitization of user-supplied input before using in SQL queries, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPKit Multiple SQL Injection CAN-2005-2683	Medium	Security Focus, Bugtraq ID: 14629, August 22, 2005
PhpOutsourcing Zorum 3.5	A vulnerability has been reported in the '/Zorum/prod.php' script due to insufficient validation of the 'argv' parameter, which could let a remote malicious user execute arbitrary PHP code. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Zorum Input Validation CAN-2005-2651 CAN-2005-2652	High	Security Tracker Alert ID: 1014725, August 18, 2005
phpPgAds phpPgAds 2.0.5	Multiple vulnerabilities have been reported: a vulnerability was reported because a vulnerable version of XML-RPC for PHP was used, which could let a remote malicious user execute arbitrary PHP code; an SQL injection vulnerability was reported in 'lib-view-direct.inc.php' due to insufficient sanitization of the 'clientid' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported due to insufficient verification of certain parameters before used to include files, which could let a remote malicious user include arbitrary local files. Upgrades available at: http://prdownloads. sourceforge.net/ phppgads/ phpPgAds-2.0.6. tar.gz?down load There is no exploit code required; however, a Proof of Concept exploit has been published.	phpPgAds Multiple Vulnerabilities CAN-2005-2636 CAN-2005-2635 CAN-2005-2498	High	Secunia Advisory: SA16469, August 17, 2005
PostNuke Development Team PostNuke 0.76 RC4b	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and an SQL injection vulnerability was reported in 'DL-viewdownload.PHP' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PostNuke Multiple Cross-Site Scripting & SQL Injection	Medium	Security Focus Bugtraq ID: 14635 & 14636, August 22, 2005
PowerDNS PowerDNS 2.x	Several vulnerabilities have been reported: a remote Denial of Service vulnerability was reported in the LDAP backend due to insufficient validation of user-supplied queries; and a remote Denial of Service vulnerability was reported due to an error when handling requests that are denied recursion. Update available at: http://www.powerdns.com/ downloads/ Debian: http://security.debian.org/ pool/updates/main/p/pdns/ Debian: http://security.debian.org/ pool/updates/main/ **SUSE:** **ftp://ftp.suse.com** **/pub/suse/** Currently we are not aware of any exploits for these vulnerabilities.	PowerDNS Denials of Service CAN-2005-2301 CAN-2005-2302	Low	Secunia Advisory: SA16111, July 18, 2005 Debian Security Advisory, DSA 771-1, August 1, 2005 Debian Security Advisory, DSA 773-1, August 11, 2005 **SUSE Security Summary Report, SUSE-SR:2005:019, August 22, 2005**
RunCMS RunCMS 1.2 & prior	Several vulnerabilities have been reported: a vulnerability was reported in '/includes/common.php' due to incorrect usage of the 'EXTR_OVERWRITE' argument in the 'extract()' function, which could let a remote malicious user overwrite arbitrary variables; and an SQL injection was reported in 'newbb_plus/newtopic.php,' 'newbb_plus/edit.php,' and 'newbb_plus/reply.php' due to insufficient sanitization of the 'forum' parameter and in 'messages/print.php' due to insufficient sanitization of the 'msg_id' parameter before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. The vulnerabilities were reportedly silently patched in mid July. There is no exploit code required; however, a Proof of Concept exploit has been published.	RunCMS SQL Injection &Arbitrary Variable Overwrite	Medium	Secunia Advisory: SA16514, August 23, 2005
SquirrelMail SquirrelMail 1.4.0-1.4.5-RC1.	A vulnerability has been reported in 'options_identities.php' because parameters are insecurely extracted, which could let a remote malicious user execute arbitrary HTML and script code, or obtain/manipulate sensitive information. Upgrades available at: http://www.squirrelmail.org/ download.php Debian: http://security.debian.org/ pool/updates/main/s/ squirrelmail/	SquirrelMail Variable Handling CAN-2005-2095	High	GulfTech Security Research Advisory, July 13, 2005 Debian Security Advisory, DSA 756-1, July 13, 2005 RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005

	RedHat: http://rhn.redhat.com/errata/RHSA-2005-595.html Apple: http://docs.info.apple.com/article.html?artnum=302163 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.			Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 **Fedora Update Notifications, FEDORA-2005-779 & 780 , August 22, 2005**
SquirrelMail SquirrelMail 1.4.0 through 1.4.4	Multiple vulnerabilities have been reported that could let remote malicious users conduct Cross-Site Scripting attacks. Upgrade to 1.4.4 and apply patch: http://prdownloads.sourceforge.net/squirrelmail/sqm-144-xss.patch Gentoo: http://security.gentoo.org/glsa/glsa-200506-19.xml Mandriva: http://www.mandriva.com/security/advisories Debian: http://security.debian.org/pool/updates/main/s/squirrelmail/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-595.html Apple: http://docs.info.apple.com/article.html?artnum=302163 **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/** There is no exploit code required.	SquirrelMail Cross-Site Scripting Vulnerabilities CAN-2005-1769	Medium	SquirrelMail Advisory, June 15, 2005 Gentoo Linux Security Advisory, GLSA 200506-19, June 21, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:108, July 1, 2005 Debian Security Advisory , DSA 756-1, July 13, 2005 RedHat Security Advisory, RHSA-2005:595-12, August 3, 2005 Apple Security Update 2005-007, APPLE-SA-2005-08-15, August 15, 2005 **Fedora Update Notifications, FEDORA-2005-779 & 780 , August 22, 2005**
Topic Board PHPTB Topic Board 2.0	Multiple remote file include vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary server-side script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	PHPTB Topic Board Multiple Remote File Include CAN-2005-2633	High	Security Focus, Bugtraq ID 14592, August 17, 2005
Virtual Edge Netquery 3.11	A vulnerability has been reported in the 'nquser.php' script due to insufficient validation of the 'host' parameter, which could let a remote malicious user execute arbitrary code. Update available at: http://www.xoops.org/modules/news/article.php?storyid=2471 There is no exploit code required.	Netquery Input Validation CAN-2005-2684	High	Security Tracker Alert ID: 1014750, August 22, 2005
W-Agora W-Agora 4.2	A Directory Traversal vulnerability has been reported in the 'Site' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	W-Agora 'Site' Parameter Directory Traversal CAN-2005-2648	Medium	Security Focus, Bugtraq ID 14597, August 18, 2005
Woltlab Burning Board 2.2.2/2.3.3 & prior	An SQL injection vulnerability has been reported in the 'ModCP.php' script due to insufficient sanitization of the 'x' and 'y' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	Woltlab Burning Board SQL Injection CAN-2005-2673	Medium	Security Tracker Alert ID: 1014746, August 21, 2005

Xerox Xerox Document Centre	Multiple vulnerabilities have been reported: a vulnerability was reported due to unspecified errors, which could let a remote malicious user bypass authentication; a remote Denial of Service vulnerability was reported when handling HTTP requests; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. Patches available at: http://www.xerox.com/downloads/usa/en/c/cert_P24_MicroServer_Web_Serve r_Patch.zip There is no exploit code required.	Xerox MicroServer Web Server Multiple Authentication Bypass & Input Validation CAN-2005-2645 CAN-2005-2646 CAN-2005-2647	Medium	XEROX Security Bulletin, XRX05-008 & 009, August 17, 2005

[back to top]

Wireless

The section below contains wireless vulnerabilities, articles, and viruses/trojans identified during this reporting period.

- **India bypasses the wires to bring Wi-Fi to its remote residents:** In several developing countries, including India, wireless technology is making universal Internet access an attainable goal. Source: http://www.csmonitor.com/2005/0819/p07s01-wosc.html

Wireless Vulnerabilities

- BlueZ Arbitrary Command Execution: A vulnerability has been reported due to insufficient sanitization of input passed as a remote device name, which could let a remote malicious user execute arbitrary code.
- BluezHCIDpwned.txt**:** Document that outlines an exploitable scenario for the BlueZ vulnerability.

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
August 21, 2005	solaris_lpd_unlink.pm	Yes	Exploit for the Sun Solaris Printd Arbitrary File Deletion vulnerability.
August 20, 2005	Elm-expires.c	Yes	Script that exploits the Elm 'Expires' Header Remote Buffer Overflow vulnerability.
August 20, 2005	procexp_exp.exe	No	Proof of Concept exploit for the Sysinternals Process Explorer CompanyName Value Buffer Overflow vulnerability.
August 19, 2005	gtchatDoS.txt	No	Remote Denial of Service exploit for the GTChat vulnerability.
August 19, 2005	IE-Msddsdll-0day.txt	Yes	Microsoft Internet Explorer msdds.dll remote code execution exploit.
August 18, 2005	aircrack-2.23.tgz	N/A	An 802.11 WEP cracking program that can recover a 40-bit or 104-bit WEP key once enough encrypted packets have been gathered.
August 18, 2005	BluezHCIDpwned.txt	N/A	Document that outlines an exploitable scenario for hcid using the popen() bug in security.c.
August 18, 2005	chmpokbof.zip	No	Proof of Concept exploit for the Chris Moneymaker's World Poker Championship Buffer Overflow vulnerability.
August 18, 2005	msnPass.txt	N/A	MSN Messenger password decrypter for Microsoft Windows XP and 2003.
August 18, 2005	phpAdsNew205.txt	Yes	Detailed exploitation for the phpAdsNew and phpPgAds vulnerabilities.
August 18, 2005	Zorum-rem_code.php zorum.html	No	Scripts that exploits the Zorum Input Validation vulnerability.
August 17, 2005	browser_ident.pdf	N/A	White paper discussing web browser identification and how proper identification can enable a remote site to know what attacks to use against a visitor.
August 17, 2005	bypassing-win-heap-protections.pdf	N/A	A whitepaper that describes a new way to bypass Microsoft Windows heap protection mechanisms.
August 17, 2005	IE-Msddsdll-0day.pl	No	Exploit for the Microsoft Visual Studio .NET msdds.dll Remote Code Execution vulnerability.
August 17, 2005	kismet-2005-08-R1.tar.gz	N/A	An 802.11 layer 2 wireless network sniffer that is capable of sniffing using almost any wireless card supported in Linux.
August 17, 2005	nmap-3.83.DC13.tgz	N/A	A utility for port scanning large networks and single hosts.
August 17, 2005	sakeru.txt	N/A	Proof of Concept tool that exploits a weakness in Websense.
August 17, 2005	x_osh2.pl.txt	No	New version of the Operator Shell (osh) 1.7-12 local root vulnerability.
August 14, 2005	Win2000-MS05-039.c HOD-ms05039-pnp-expl.c	Yes	Scripts that exploit the Microsoft Plug and Play Arbitrary Code Execution or Elevated Privileges vulnerability.

[back to top]

Trends

- **US tops poll of spyware purveyors:** According to a study by Webroot Software, the majority of spyware is coming from the US, with Poland in second, and the Netherlands third. Spyware purveyors are expanding their distribution channels and adopting new tactics in a bid to cash-in by infecting more PCs with parasitic malware. Source: http://www.theregister.co.uk/2005/08/23/webroot_spyware_report/ .
- **Storm brewing over SHA-1 as further breaks are found:** An attack on the Secure Hash Algorithm, an encryption standard frequently used to digitally sign documents, has been refined by three Chinese researchers. This attack was presented last week at the Crypto conference. Source: http://www.securityfocus.com/news/11292
- **Exploit for Vulnerability in Microsoft DDS Library Shape Control (msdds.dll) component:** US-CERT is aware of a public exploit for a vulnerability in the Microsoft DDS Library Shape Control (msdds.dll) component, which comes with various Microsoft products such as Visual Studio .NET and Microsoft Office. Systems with Visual Studio .NET 2002, which installs msdds.dll version 7.0.9466.0, are vulnerable. Source: http://www.us-cert.gov/current/.
- **"Stealthy" Worms, Trojans Seen Tripling In Number:** According to Kaspersky Labs, attackers are increasingly turning to stealthy rootkits to keep anti-virus vendors from detecting and deleting malicious worms or Trojan horses."Over the last 12 months, we've seen a large jump in the use of rootkits," said David Emm, a senior technology consultant with Kaspersky Labs. Source: http://www.techweb.com/wire/security/169500359.
- **Over 90 Percent Of Companies Regularly Expose Employee, Customer Data:** According to a recent study by Reconnex, an enterprise risk management vendor, 91 percent of companies exposed credit card numbers, and 82 percent exposed employee Social Security numbers. "We are seeing evidence of a growing trend regarding the distribution of sensitive data via Webmail," said the index's report. Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=A2VZY02Q0OCXUQSNDBCSKH0CJUMEKJVN?articleID=169500368.
- **Hacker underground erupts in virtual turf wars:** Viruses are now designed to kill any other competing viruses in computer systems. That's a major reason that turf wars are emerging among hackers. Source: http://www.csmonitor.com/2005/0822/p01s01-stct.html.
- **Search Engines Find Stolen Identities:** During the first six months of 2005, more than 50 million identities were lost or stolen in a series of high profile data breaches across the United States. Thanks to search engines, many can be easily found. Source: http://www.informationweek.com/story/showArticle.jhtml;jsessionid=DCREHOUZ5L3EMQSNDBCSKH0CJUMEKJVN?articleID=169400258.
- **Consumer worries about online security on the rise:** According to a survey released by RSA Security Inc. and LightSpeed Research, more than four-fifths of 8,000 consumers felt threatened or extremely threatened by online fraud and identify theft. This includes all type of online transactions, including securities trading, banking, auctions, and retail. Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=QHNJND24A1HTWQSNDBCCKHSCJUMEKJVN?articleID=169400081.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trend	Date	Description
1	Netsky-P	Win32 Worm	Stable	March 2004	A mass-mailing worm that uses its own SMTP engine to send itself to the email addresses it finds when scanning the hard drives and mapped drives. The worm also tries to spread through various file-sharing programs by copying itself into various shared files.
2	Mytob.C	Win32 Worm	Slight Increase	March 2004	A mass-mailing worm with IRC backdoor functionality which can also infect computers vulnerable to the Windows LSASS (MS04-011) exploit. The worm will attempt to harvest email addresses from the local hard disk by scanning files.
3	Zafi-D	Win32 Worm	Slight Decrease	December 2004	A mass-mailing worm that sends itself to email addresses gathered from the infected computer. The worm may also attempt to lower security settings, terminate processes, and open a back door on the compromised computer.
4	Netsky-Q	Win32 Worm	Stable	March 2004	A mass-mailing worm that attempts to launch Denial of Service attacks against several web pages, deletes the entries belonging to several worms, and emits a sound through the internal speaker.
5	Mytob-BE	Win32 Worm	Slight Decrease	June 2005	A slight variant of the mass-mailing worm that utilizes an IRC backdoor, LSASS vulnerability, and email to propagate. Harvesting addresses from the Windows address book, disabling antivirus, and modifying data.
6	Mytob-AS	Win32 Worm	Stable	June 2005	A slight variant of the mass-mailing worm that disables security related programs and processes, redirection various sites, and changing registry values. This version downloads code from the net and utilizes its own email engine.
7	Zafi-B	Win32 Worm	Increase	June 2004	A mass-mailing worm that spreads via e-mail using several different languages, including English, Hungarian and Russian. When executed, the worm makes two copies of itself in the %System% directory with randomly generated file names.
8	Netsky-D	Win32 Worm	Slight Increase	March 2004	A simplified variant of the Netsky mass-mailing worm in that it does not contain many of the text strings that were present in NetSky.C and it does not copy itself to shared folders. Netsky.D spreads itself in e-mails as an executable attachment only.

9	Netsky-Z	Win32 Worm	Decrease	April 2004	A mass-mailing worm that is very close to previous variants. The worm spreads in e-mails, but does not spread to local network and P2P and does not uninstall Bagle worm. The worm has a backdoor that listens on port 665.
10	Lovgate.w	Win32 Worm	Decrease	April 2004	A mass-mailing worm that propagates via by using MAPI as a reply to messages, by using an internal SMTP, by dropping copies of itself on network shares, and through peer-to-peer networks. Attempts to access all machines in the local area network.

Table Updated August 20, 2005

[back to top]

Last updated August 25, 2005